SPYWOLF

Security Audit Report

Completed on

April 19, 2023

OVERVIEW

This audit has been prepared for **EARN PROTOCOL** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

EARN PROTOCOL

PROJECT DESCRIPTION

According to their whitepaper:

Earn Protocol is a platform designed to make it easy for users to participate in yield farming, staking, and liquidity pooling. Yield farming allows users to earn rewards for supplying their capital and liquidity to decentralized financial applications on Binance-based networks.

Release Date: Presale starts in April, 2023

Category: DeFi

CONTRACT INFO

Token Name
Earn Protocol

Symbol
EARN

Contract Address
0x1E33F65E7ddC50bF195cfde6abAeD25370d2D32f

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Apr 17, 2023

Verified?
Yes

Total Supply
10,000,000,000

Status
Launched

TAXES

Buy Tax
7.5%

Sell Tax
7.5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	0
Uniq Senders	0
Uniq Receivers	0
Total Amount	0 EARN
Median Transfer Amount	0 EARN
Average Transfer Amount	0 EARN
First transfer date	N/A
Last transfer date	N/A
Days token transferred	0

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-04-17 21:24:29 UTC
Created	2023-04-17 21:24:29 UTC
Create TX	0x2e8dd070c25e8bf8807a1b7e266432eb0e84d6547e76a3e2ee5bc3f0bde617d1
Creator	0x532adcb4f0654f400346acc6a8eed8b88713eb74

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can mint (create) new tokens.
This can lead to token's rapid inflation and liquidity drain.

```
function mint(address _to, uint256 _amount) public onlyOwner {
    _mint(_to, _amount);
}

function _mint(address account, uint256 amount) internal virtual {
    require(account != address(0), "ERC20: mint to the zero address");

    _beforeTokenTransfer(address(0), account, amount);

    _totalSupply += amount;
    unchecked {
        _balances[account] += amount;
    }
    emit Transfer(address(0), account, amount);

    _afterTokenTransfer(address(0), account, amount);
}
```

- Recommendation:
  - Considered as good practice to not allow new tokens to be created after initial token generation event (TGE).

FOUND THREATS

⚠ High Risk

Owner can enable/disable trading.
When such restriction is in place, no further token transfers will be allowed for non excluded addresses.

```
function UpdateSwapEnabled(bool _enabled) public onlyOwner {
    emit SwapEnabledUpdated(msg.sender, _enabled);
    swapEnabled = _enabled;
}

modifier antiWhale(address sender, address recipient, uint256 amount) {
    if (maxTransferAmount() > 0) {
        if (
            _excludedFromAntiWhale[sender] == false
            && _excludedFromAntiWhale[recipient] == false
        ) {
            require(amount <= maxTransferAmount(),
            "EARN::antiWhale: Transfer amount exceeds the maxTransferAmount");
            require(swapEnabled == true, "EARN::swap: Cannot transfer at the moment");
        }
    }
    _;
}

function _transfer(address sender, address recipient, uint256 amount)
internal virtual override antiWhale(sender, recipient, amount) {
.....................
}
```

- Recommendation:
    - Considered as good practice to be unable to pause/stop the contrat once launched.

FOUND THREATS

⚠ High Risk

Owner can change contract's auto swap settings.
If minAmountToLiquify is set to 0 or very low number and swapAndLiquifyEnabled is set to true and contract's balances are 0, contract will halt when user sell/transfer tokens, making it impossible to sell.

```
function updateSwapAndLiquifyEnabled(bool _enabled) public onlyOperator {
    emit SwapAndLiquifyEnabledUpdated(msg.sender, _enabled);
    swapAndLiquifyEnabled = _enabled;
}

function updateMinAmountToLiquify(uint256 _minAmount) public onlyOperator {
    emit MinAmountToLiquifyUpdated(msg.sender, minAmountToLiquify, _minAmount);
    minAmountToLiquify = _minAmount;
}

function swapAndLiquify() private lockTheSwap transferTaxFree {
    uint256 contractTokenBalance = balanceOf(address(this));
    uint256 maxTx = maxTransferAmount();
    contractTokenBalance = contractTokenBalance > maxTx ? maxTx : contractTokenBalance;

    if (contractTokenBalance >= minAmountToLiquify) {
        uint256 liquifyAmount = minAmountToLiquify;
        uint256 half = liquifyAmount.div(2);
        uint256 otherHalf = liquifyAmount.sub(half);
        uint256 initialBalance = address(this).balance;
        swapTokensForEth(half);
        uint256 newBalance = address(this).balance.sub(initialBalance);
        addLiquidity(otherHalf, newBalance);
        emit SwapAndLiquify(half, newBalance, otherHalf);
    }
}
```

- Recommendation:
  - Ensure that minAmountToLiquift is always above 1 token, considering token's decimals.

FOUND THREATS

⚠ Low Risk

Owner can set max transaction limit but cannot lower it than 0.01% of total supply.

```
function setExcludedFromAntiWhale(address _account, bool _excluded) public onlyOperator {
    _excludedFromAntiWhale[_account] = _excluded;
}


function updateMaxTransferAmountRate(uint16 _maxTransferAmountRate) public onlyOperator {
    require(_maxTransferAmountRate <= 10000,
    "EARN::updateMaxTransferAmountRate: Max transfer amount rate must not exceed the maximum rate.");
    emit MaxTransferAmountRateUpdated(msg.sender, maxTransferAmountRate, _maxTransferAmountRate);
    maxTransferAmountRate = _maxTransferAmountRate;
}

function maxTransferAmount() public view returns (uint256) {
    return totalSupply().mul(maxTransferAmountRate).div(10000);
}

modifier antiWhale(address sender, address recipient, uint256 amount) {
    if (maxTransferAmount() > 0) {
        if (
            _excludedFromAntiWhale[sender] == false
            && _excludedFromAntiWhale[recipient] == false
        ) {
            require(amount <= maxTransferAmount(),
            "EARN::antiWhale: Transfer amount exceeds the maxTransferAmount");
            require(swapEnabled == true, "EARN::swap: Cannot transfer at the moment");
        }
    }
    _;
}

function _transfer(address sender, address recipient, uint256 amount)
internal virtual override antiWhale(sender, recipient, amount) {
.....................
}
```

- Recommendation:
  - When max transaction limitations are applied, max transaction amount should be not lower than 0.1% of total supply.

Informational

Owner can exclude address from max transaction limit and trade disable restrictions.

```
function setExcludedFromAntiWhale(address _account, bool _excluded) public onlyOperator {
    _excludedFromAntiWhale[_account] = _excluded;
}
```

IMPORTANT
No initial supply is minted in contract's creation.
Token's total supply is 0.

Total Supply: 0 EARN

```
contract EarnProtocol is ERC20, Ownable {
.................
constructor() ERC20("Earn Protocol", "EARN") {
    _operator = _msgSender();
    emit OperatorTransferred(address(0), _operator);

    _excludedFromAntiWhale[msg.sender] = true;
    _excludedFromAntiWhale[address(0)] = true;
    _excludedFromAntiWhale[address(this)] = true;
    _excludedFromAntiWhale[BURN_ADDRESS] = true;
}
.................
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Earn Protocol

GOOD PRACTICES FOUND

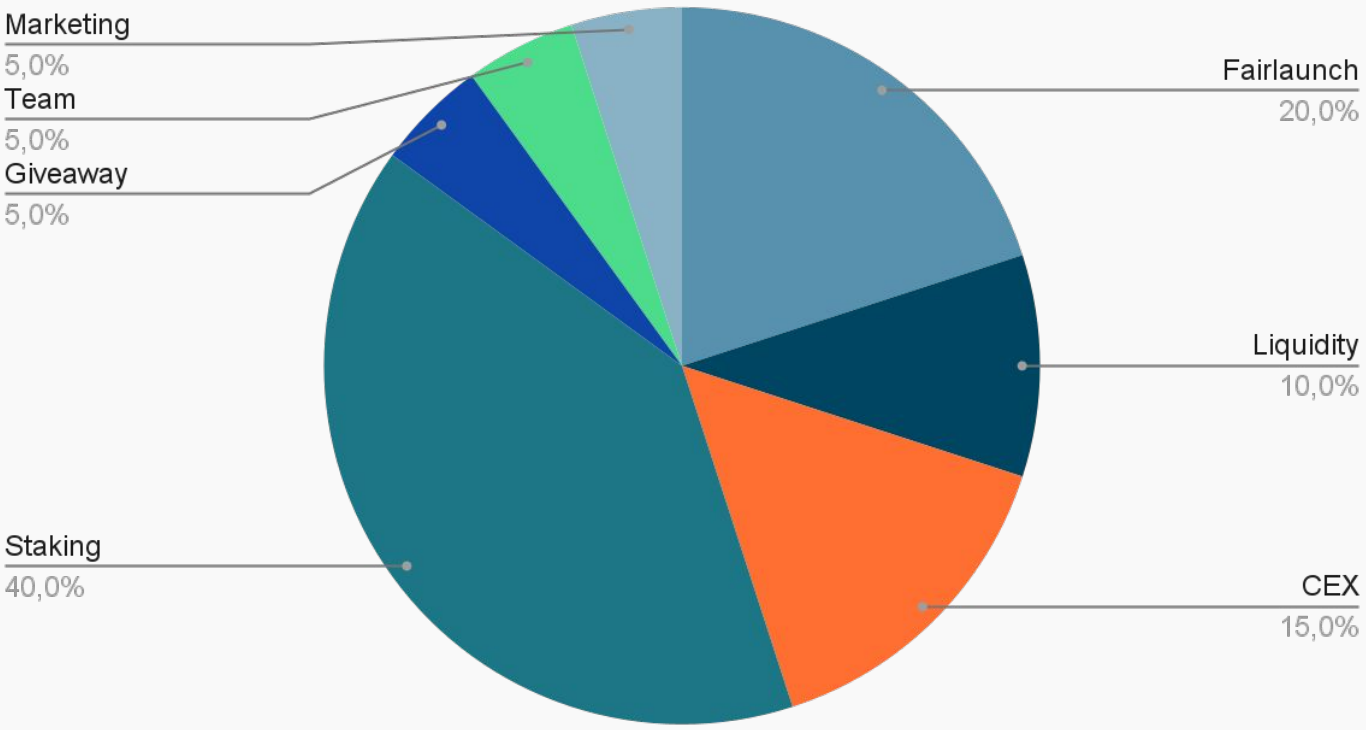
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 20% - Fairlaunch
- 10% - Liquidity
- 15% - CEX
- 5% - Giveaway
- 40% - Staking
- 5% - Team
- 5% - Marketing

Tokens distribution



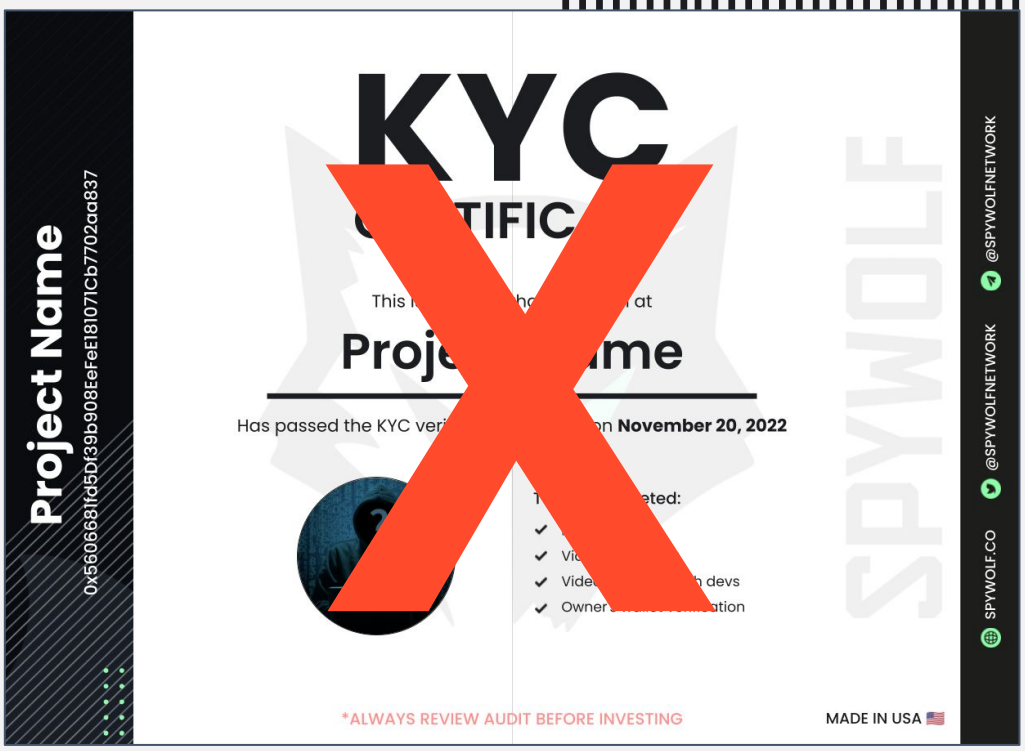
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://earnprotocol.org/

Domain Registry
https://www.namecheap.com

Domain Expiration
2024-04-01

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

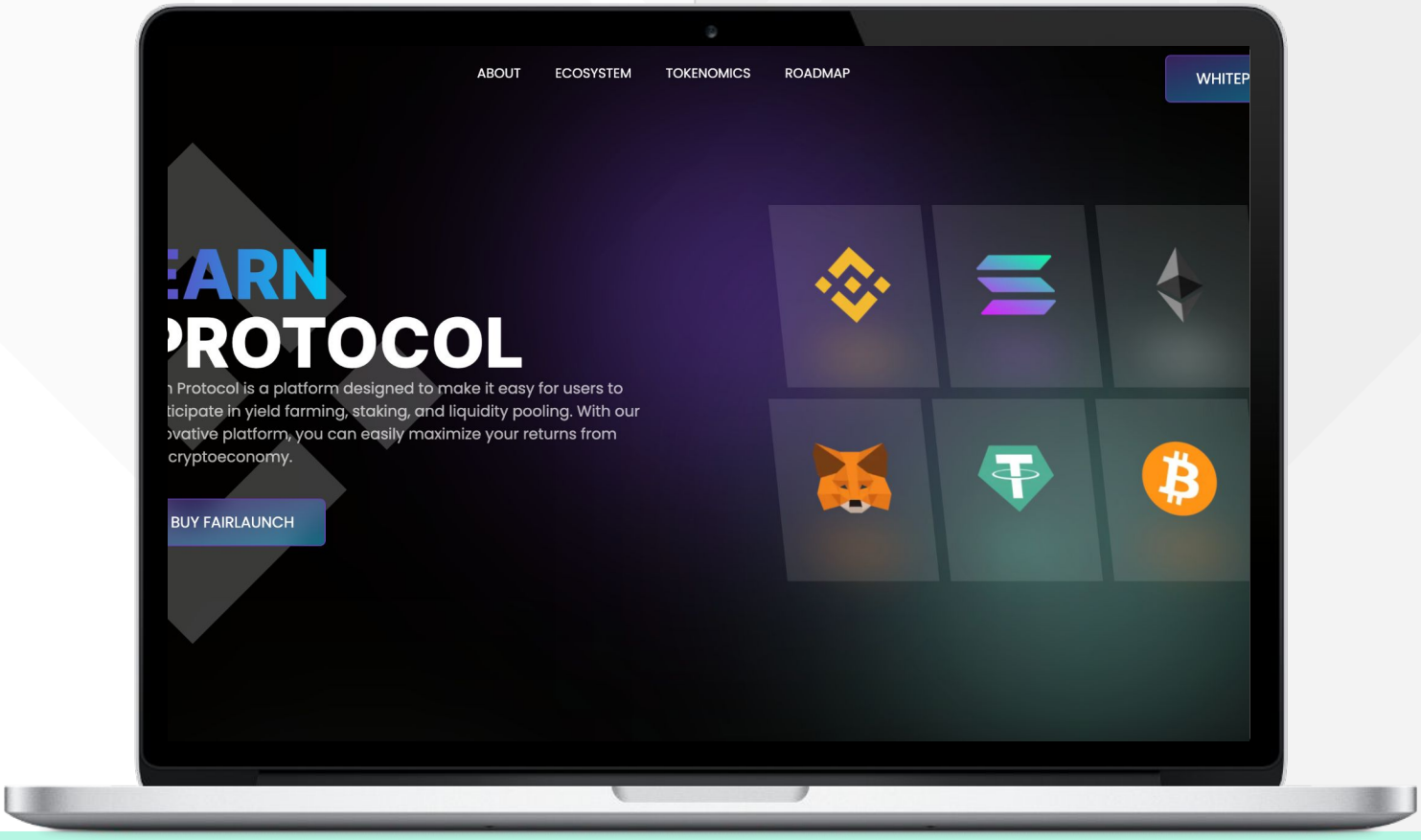
Design
Very nice design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found
.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



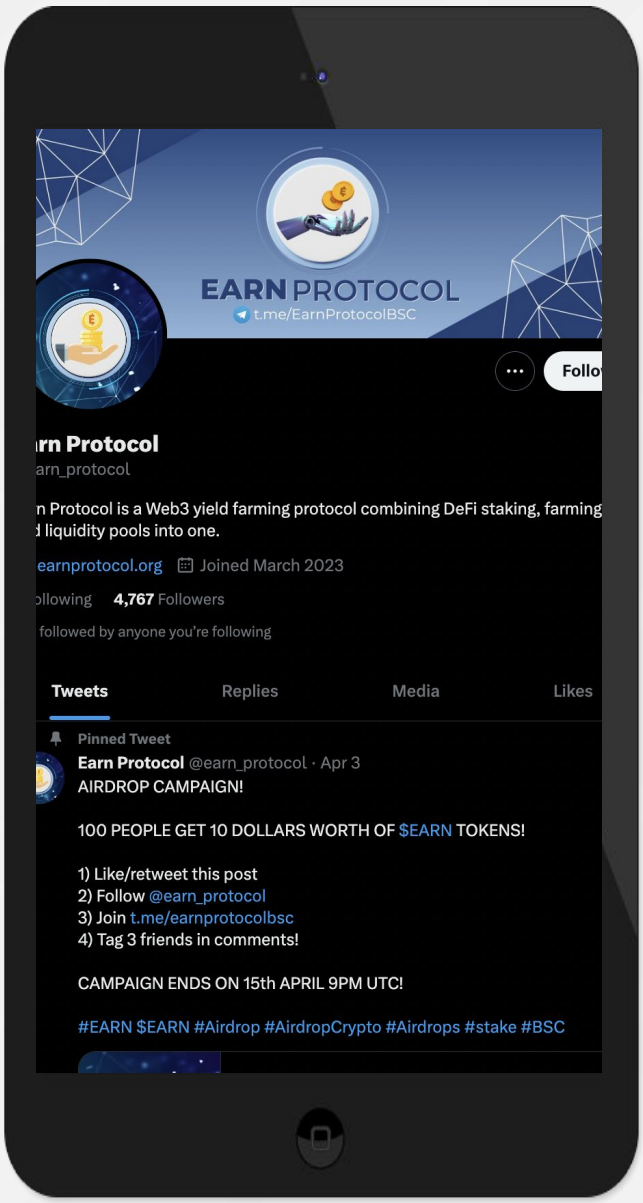
earnprotocol.org

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter

@earn_protocol

- 4 770 followers
- 4 total posts
- Posts once every few days

Discord

- Not available

Telegram

@TelegramUSERNAME

- 3 438 members
- Active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.